

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

INFORMATION ASSOCIATED WITH  
JISROFF@UMSWI.COM, JSWEET@UMSWI.COM,  
AND MPFLEGER@UMSWI.COM THAT IS STORED  
AT PREMISES OWNED, MAINTAINED,  
CONTROLLED, OR OPERATED BY MICROSOFT  
CORPORATIONCase No. 20-MJ-20

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711:

See Attachment B.

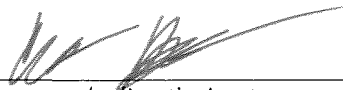
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

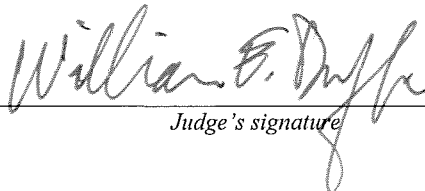
The search is related to violations of:

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signatureColleen Brennan, FBI Special Agent  
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 2/6/2020  
Judge's signatureCity and State: Milwaukee, WisconsinHonorable William E. Duffin, U.S. Magistrate Judge  
Printed Name and Title

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Colleen Brennan, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises controlled by Microsoft Corporation ("Microsoft"), an email provider headquartered at Microsoft Corporation, One Microsoft Way, Redmond, WA 98052. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since March 2019. I am currently assigned to the White Collar Squad of the Milwaukee Field Office, where I primarily investigate crimes concerning bank fraud, wire fraud, money laundering and civil rights violations. Prior to working for the FBI, I worked for approximately four years at SAP, a multinational software corporation, and I also worked for approximately one year as a registered representative for Primerica Financial Services. I received a Bachelor's degree from Columbia University, majoring in Political Science with a concentration in Business Management.

3. As a Special Agent, I received federal law enforcement training at the FBI Academy in Quantico, VA. My training at the FBI Academy included experience in interviewing

and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, evidence identification, and various other criminal laws and procedures. I have received training in investigating violations of federal statutes, including those involving civil rights, cyber, bank fraud and wire fraud. While involved with these types of investigations, I have worked extensively with agents who specialize or have expertise in these areas.

4. I spent my career at SAP working directly with companies going through enterprise software implementations. In my role as an Account Executive, I partnered with employees of companies new to SAP systems to identify which learning and enablement tools could best increase the efficiency of their software platform. The training I received at SAP entailed hands on development of cloud computing systems, customer engagement strategies, and value based selling techniques.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code, § 1344 (bank fraud), and Title 18 United States Code, §1349 (attempt and conspiracy) have been committed by employees of United Milwaukee Scrap, including former CEO Jeffrey Isroff and CFO Jeffrey Sweet. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

#### **JURISDICTION**

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

**PROBABLE CAUSE**

8. The information detailed in this affidavit is based on my personal knowledge and observations, bank records, UMS business records, information from other law enforcement agencies, and third party witnesses. I believe these sources of information to be credible and reliable based on the corroboration of the information and my experience with these matters. The information in this affidavit does not include all of my knowledge and investigation into this case. These facts are presented for the sole purpose of establishing probable cause in support of the application for a search warrant.

9. United Milwaukee Scrap Holdings, LLC (“UMS”) buys, processes, and sells scrap metals generated from industry, obsolete materials, plant tear downs, construction, and other sources. UMS purchases scrap metal and then recovers valuable metals (including iron, aluminum, and copper) from the scrap metal. UMS then sells the valuable metals for a profit. UMS’s subsidiaries include United Milwaukee Scrap, LLC, Schulz’s Recycling, Inc., United MFR, LLC, United Milwaukee Scrap International Sales Corporation, and UMS Trucking, LLC.

10. According to the Wisconsin Department of Financial Institutions, the registered effective date of UMS was September 24, 2013. The “principal office” is listed as 3100 West Concordia Avenue in Milwaukee, Wisconsin.

11. UMS regularly used cash to buy scrap metal from the public.

12. BMO Harris Bank and UMS Holdings, LLC executed a credit agreement on or about September 28, 2018. BMO Harris provided UMS with a revolving line of credit for a maximum of \$35 million under the credit agreement, and a term loan of \$4 million. Associated

Bank was a participant in this loan. Associated Bank had a longer lending relationship with UMS and had been providing a line of credit to UMS since at least 2015. Part of the collateral for the revolving line of credit for both the BMO Harris and the Associated Bank loans was UMS's scrap metal inventory. BMO Harris and Associated Bank are federally insured financial institutions.

13. Jeffrey Isroff ("Isroff") was the CEO of UMS from approximately October of 2013 until his resignation in early 2019. Isroff received a base salary of \$300,000 from UMS according to his October 2013 employment agreement. He also was eventually provided with an approximately \$800,000 personal loan from UMS. Over time, Isroff has paid back approximately \$400,000 of the \$800,000 principal by having UMS use his bonuses to pay back the principal on the personal loan. According to his 2018 W-2 personal federal income tax document, Isroff's 2018 income was approximately \$447,000.

14. Mark Pfleger is currently the Vice President of Operations for UMS. Jeff Sweet was the Vice President of Finance at UMS in 2015 through the present. Arthur Arnstein has an equity interest in UMS Holdings, LLC. Arthur Arnstein's sons, David and Daniel, also worked for UMS.

15. In February of 2019, Silverman Consulting was contacted by BMO Harris because UMS was not performing well on its loan. Silverman Consulting is a Chicago-based consulting firm that specializes in management advisory and restructuring services. Since the firm's inception in 1978, Silverman Consulting has helped to engineer the turnaround of more than 700 public and privately held businesses ranging in size from \$5 million to over \$1.2 billion in annual revenues.

16. Silverman Consulting determined that UMS had been fraudulently overstating the value of its inventory to BMO Harris and Associated Bank. UMS provided Borrowing Base Certificates to its lenders on a regular basis, and on these Borrowing Base Certificates, the value

of the inventory was overstated.

17. Many of the Borrowing Base Certificates are signed by Jeff Sweet. BMO Harris required the Borrowing Base Certificates to be submitted as part of the loan agreement. Given the inventory was an important part of the collateral for the loan, it was important for the lenders to know the accurate value of this collateral.

18. Silverman Consulting has stated that on a monthly basis, Sweet provided Isroff with the numbers that detailed the size of the inventory. Isroff would then make changes to the inventory numbers and provide the altered numbers to Sweet. Silverman Consulting's analysis indicated the fraudulent altering of the value of UMS's inventory began in approximately 2015, when the price of scrap metal sold by UMS decreased significantly.

19. In 2015, UMS lost approximately \$5 million. Silverman consulting estimates UMS lost approximately \$500,000 per month from 2016 through 2018.

20. Silverman Consulting's CEO, Michael Silverman ("Silverman"), spoke to Isroff in early February 2019. Isroff stated that UMS's inventory could be overstated by approximately \$200,000 to \$300,000. On February 11, 2019, Isroff resigned from UMS. In the afternoon of February 11, 2019, Silverman spoke with Sweet and Pfleger. Sweet told Silverman that the inventory could be misstated by as much as 25%. Pfleger believed the inventory was overstated by about 50%.

21. Beginning on April 30, 2019, a physical inventory was conducted and UMS weighed all of its inventory. The inventory process took 3 days. This inventory showed that UMS had \$9 million in inventory on hand. UMS's ledger showed it had \$26 million in inventory on hand. Thus the ledger was overstated by a figure of approximately \$17 million.

22. On January 31, 2019, Sweet submitted a Borrowing Base Certificate to the lenders

that stated the value of the inventory for UMS was over \$28 million dollars. On February 28, 2019, after Isroff had resigned, Sweet submitted a Borrowing Base Certificate to the lenders that stated the value of the inventory was only \$13.7 million. This same Borrowing Base Certificate indicates that UMS's gross sales in February 2018 were only \$486,94.96. The January 31, 2019 Borrowing Base Certificate thus contains a false accounting for the value of the inventory. On February 26, 2019, BMO Harris sent UMS a default notice, stating that a materially false Borrowing Base Certificate submitted on or about February 12, 2019 resulted in one or more Events of Default under the September 28, 2018 Credit Agreement. BMO Harris employees stated that Borrowing Base Certificates were submitted via email.

23. Silverman Consulting estimates the total losses on the loans to be as much as \$15 million.

24. UMS was dependent on its line of credit in order to operate. UMS needed the banks' money to run its business and purchase scrap metal. If Isroff had reported to the banks that UMS was losing \$6 million per year and the true size of the inventory, UMS likely would have had its revolving line of credit pulled by the banks, and UMS likely would not have been able to continue to operate its business.

25. Silverman Consulting has been running UMS since approximately February of 2019, with Silverman acting as UMS's CEO.

26. A Silverman Consulting employee stated he took computer hardware out of Isroff's office, and the FBI took custody of this computer software on November 26, 2019.

27. On July 18, 2019, a Grand Jury subpoena was sent to UMS Holdings, LLC (served on Silverman, the acting CEO of UMS) requesting a variety of financial records, loan records, records related to inventory, and email communications from or to Isroff, Sweet, and Pflieger that



contained certain keywords or discussed certain topics relevant to the investigation.

28. UMS provided a large quantity of emails to the FBI. However, not all emails from the UMS employees were provided to the FBI. Also, I note that Silverman Consulting has indicated to the FBI that Jeff Sweet was involved in determining what documents were sent to the FBI pursuant to the subpoena sent to UMS Holdings, LLC. More broadly, it appeared that the FBI had not received all of the documents requested in the Grand Jury subpoena.

29. On November 26, 2019, a search warrant was executed at the UMS headquarters located at 3100 West Concordia Avenue in Milwaukee, WI. The FBI seized financial, loan, and inventory documents and other evidence, including computers and electronic media. The FBI also imaged UMS servers in the UMS headquarters building the day of the search.

30. Through both the grand jury subpoena and the search warrant, the FBI has obtained some emails relevant to the investigation. For example, on May 14, 2018, Isroff used his **jisroff@umswi.com** email account to email Sweet at **jsweet@umswi.com**, and gave him a list of adjustments that should be made to the inventory numbers. On May 24, 2018, Isroff used his **jisroff@umswi.com** email account to email Sweet at **jsweet@umswi.com**, a spreadsheet titled “UMS Inventory Book v Physical . . .” and told Sweet to send him a preliminary Profit and Loss statement using that inventory. In other emails, Sweet requests actual inventory numbers from employees that actually work in the scrap yards. In other emails, Sweet discusses conducting a physical inventory of UMS’s scrap metal inventory with other employees in 2016 and 2017.

31. On January 22, 2019, Sweet used his **jsweet@umswi.com** email account to send Isroff an email at **jisroff@umswi.com**. The email contained summary inventory numbers titled “BBC” which outlined four different Borrowing Base Certificate “options”. Each Borrowing Base Certificate had different dates and numbers, and noted which had the highest asset values versus



the most cash availability. According to BMO Harris employees, there should not have been a choice as to which borrowing base certificate was filed with the bank.

32. In January 2019, Pfleger began to suspect that the inventory was overstated. He conducted an inspection of the inventory, and based on his initial estimate, the inventory was overstated by approximately \$8 million.

33. Pfleger stated that he emailed Isroff a spreadsheet detailing his findings that the inventory was overstated by approximately \$8 million. Email records show that Pfleger's business email address is **mpfleger@umswi.com**.

34. According to Pfleger, Isroff used email a lot to communicate with UMS employees, including with Pfleger.

35. Some businesses pay Microsoft for email storage service. Although the search warrant seized electronic documents from the UMS computers and servers, there is no guarantee that all relevant documents and emails were downloaded to the localized UMS computers and servers. UMS used Microsoft as its provider for email service provider.

36. In general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time.

#### **BACKGROUND CONCERNING EMAIL**

37. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail ("email") access, to the companies. Microsoft allows companies to obtain email accounts and tailor the domain names to their businesses, like the email

accounts listed in Attachment A using “umswi.com”. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

38. A Microsoft subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

39. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

40. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

41. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

42. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

### **CONCLUSION**

43. Based on the foregoing, I request that the Court issue the proposed search warrant.

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then

compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with **jisroff@umswi.com**, **jsweet@umswi.com**, and **mpfleger@umswi.com** that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at Microsoft Corporation, One Microsoft Way, Redmond, WA 98052.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Microsoft Corporation (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account January 1, 2015 to present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.



f. The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 United States Code, § 1344 (bank fraud), and Title 18 United States Code, §1349 (attempt and conspiracy), those violations involving UMS employees and occurring after January 1, 2015, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Records and information relating to a conspiracy to defraud BMO Harris and Associated Bank.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Microsoft, and my title is \_\_\_\_\_.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Microsoft. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Microsoft, and they were made by Microsoft as a regular practice; and

b. such records were generated by Microsoft's electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Microsoft in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Microsoft, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature